UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

NICOLAS KERIAZIS individually and on behalf of all others similarly situated, Plaintiff(s), v. UNITEDHEALTH GROUP INCORPORATED; UNITEDHEALTHCARE, INC.; OPTUM, INC.; and CHANGE HEALTHCARE INC.,	CASE NO.: 0:24-cv-00751 **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Nicolas Keriazis ("Plaintiff"), by and through the undersigned counsel, brings this class action complaint against Defendants UnitedHealth Group Incorporated, UnitedHealthcare, Inc., Optum, Inc., and Change Healthcare Inc. (collectively, "Defendants" or "UHG"), on behalf of himself and all others similarly situated. Plaintiff makes the following allegations based upon personal knowledge as to his own actions and upon information and belief as to all other matters:

NATURE OF THE ACTION

1. UHG, a leading global healthcare giant, faces what might be the most consequential data breach in history. A ransomware group claims to have accessed UHG's servers and seized 6 terabytes of critical confidential and highly sensitive information, resulting in network outages that have already impacted millions of patients and physicians across the country. On February 21, 2024, UHG disclosed that it was the subject of this

massive data breach whereby hackers known as "ALPHV/Blackcat" ("Blackcat") gained unauthorized access to its networks (the "Data Breach").

2. Blackcat is a notable cybergroup that infiltrates healthcare institutions' internal servers through vulnerabilities in their networks. The group uses "ransomware to identify and attack 'high-value victim institutions[.]'"[1] According to the Department of Justice, Blackcat typically steals victims' data and encrypts the institution's data, networks, and servers, blocking the institution from accessing them. The group then demands the institution pay a ransom in exchange for the keys to decrypt the institution's network and servers. In exchange for ransom, Blackcat also offers a promise that it will not publish the institution's data to Blackcat's site on the Dark Web. Still, even when ransoms are paid, this data often ends up on the Dark Web. Blackcat has emerged as the second most prolific ransomware-as-a-service variant in the world.[2]

3. Blackcat accessed, copied, and exfiltrated highly sensitive information stored on UHG's servers for millions of individuals, including active US military/navy personnel identifiable information, medical records, dental records, payment information, claims information, patients' information (such as phone numbers, addresses, Social Security

---

[1] James Farrell, *Change Healthcare Blames 'Blackcat' Group for Cyber Attack That Disrupted Pharmacies and Health Systems*, FORBES (Feb. 29, 2024, 1:18 PM), https://www.forbes.com/sites/jamesfarrell/2024/02/29/change-healthcare-blames-blackcat-group-for-cyber-attack-that-disrupted-pharmacies-and-health-systems/?sh=589769fc1c4d.

[2] *Justice Department Disrupts Prolific ALPHV/Blackcat Ransomware Variant*, DOJ (Dec. 19, 2023), https://www.justice.gov/opa/pr/justice-department-disrupts-prolific-alphvblackcat-ransomware-variant.

numbers, emails, etc.), insurance records, and more ("PHI").[3] Blackcat also encrypted portions of UHG's network, rendering them unusable.

4. The fallout from this Data Breach has and will wreak havoc on the healthcare industry. As the largest healthcare insurer, UHG processes 15 billion transactions annually, "touching one in three U.S. patient records."[4] But to stop the cybersecurity wound from bleeding further, UHG decided to take certain systems offline. Without UHG's functioning systems, the healthcare industry is immobilized. Patients are stuck in prescription purgatory without access to their vital medications. This is especially disruptive to elderly patients who have a fixed income and cannot afford medications without insurance, as well as individuals with chronic illnesses who face life-threatening symptoms without their medication. UHG's network outage is jeopardizing the health of millions of Americans.

5. Patients are not the only victims here. The ripple effect of the Data Breach is also hampering healthcare providers' practices. According to John Riggi, national advisor for cybersecurity and risk at the American Hospital Association, "… [T]his cyberattack has affected every hospital in the country one way or another."[5] Many providers are having

---

[3] *MMRG Notifies Patients of Cybersecurity Incident*, BUSINESS WIRE (Feb. 6, 2024, 5:30 PM), https://www.businesswire.com/news/home/20240206060527/en/.

[4] Nicole Sganga & Andres Triay, *Cyberattack on UnitedHealth still impacting prescription access: "These are threats to life,"* CBS NEWS (Feb. 29, 2024, 9:00 PM), https://www.cbsnews.com/news/unitedhealth-cyberattack-change-healthcare-prescription-access-still-impacted/.

[5] Nicole Sganga & Andres Triay, *Cyberattack on UnitedHealth still impacting prescription access: "These are threats to life,"* CBS NEWS (Feb. 29, 2024, 9:00 PM), https://www.cbsnews.com/news/unitedhealth-cyberattack-change-healthcare-prescription-access-still-impacted/.

trouble verifying patient eligibility and coverage, filing claims, and billing patients.[6] This leaves small and mid-sized practices especially vulnerable without normal cash flow to sustain operations. For the past ten days, these healthcare practices have not been able to receive reimbursements from insurers for patient visits. Without these reimbursements, vulnerable providers cannot afford employee payroll and medical supplies. The combination of unmedicated patients and handicapped hospitals paints a bleak future.

6. Born of UHG's negligence, patients and healthcare providers alike will feel the immediate effects of the network outage for some time. UHG's Chief Operating Officer Dirk McMahon suggests that the outage could last weeks.[7] And to make it worse, patients who had their PHI stolen will feel the sting of this Data Breach for their lifetime. All the while, Defendants continue to rake in billions of dollars off the backs of the patients and providers whose confidential and highly sensitive information they promised to protect.

7. UHG is responsible for the Data Breach because it failed to implement reasonable security procedures and practices and failed to disclose material facts surrounding its deficient security protocols.

8. As a result of UHG's failure to protect the sensitive information it was entrusted to safeguard, Plaintiff and Class members did not receive the benefit of their

---

[6] Associated Press, *Minnetonka Based United Healthcare Hacked*, KNSI (Feb. 29, 2024, 5:46 PM), https://knsiradio.com/2024/02/29/minnetonka-based-united-healthcare-hacked/.

[7] Brittany Trang, *Change Healthcare cyberattack outage could persist for weeks, UnitedHealth Group executive suggests*, STAT (Feb. 29, 2024), https://www.statnews.com/2024/02/29/change-healthcare-cyber-attack-outage-will-last-for-weeks/.

bargain with UHG and now face a significant risk of medical-related theft and fraud, financial fraud, and other identity-related fraud now and into the indefinite future.

PARTIES

9. Plaintiff Nicolas Keriazis is a California resident who fills his medical prescriptions at a local CVS Pharmacy that uses UHG's Change Healthcare platform.

10. Defendant UnitedHealth Group Incorporated is a Delaware corporation with its principal place of business in Minnetonka, Minnesota.

11. Defendant UnitedHealthcare, Inc. is a Delaware corporation with its principal place of business in Minnetonka, Minnesota.

12. Defendant Optum, Inc. is a Delaware corporation with its principal place of business in Eden Prairie, Minnesota.

13. Defendant Change Healthcare Inc is a Delaware corporation with its principal place of business in Nashville, Tennessee.

JURISDICTION AND VENUE

14. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million exclusive of interest and costs. There are more than 100 putative class members and at least some members of the proposed Class have a different citizenship from Defendants. This Court has supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367 because all claims alleged herein form part of the same case or controversy.

15. This Court has jurisdiction over UHG because it maintains and operates its headquarters in this District and/or is authorized to and does conduct business in this District.

16. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) (1) & (2) because UHG resides in this District and/or a substantial part of the events and omissions giving rise to this action occurred in this District.

FACTUAL ALLEGATIONS

Defendants' Relationship

17. UHG operates through four segments: UnitedHealthcare and three Optum segments: (1) Optum Health, (2) Optum Insight, and (3) Optum Rx (collectively, "Optum").[8]

18. According to Optum's website, Optum Health "provides care directly through local medical groups and ambulatory care systems, including primary, specialty, urgent and surgical care to nearly 103 million consumers."[9] Optum Health's customers "include employers, health systems, government and health plans."[10]

19. Optum's website states that Optum Insight "provides data, analytics, research, consulting, technology and managed services solutions to hospitals, physicians, health plans, governments and life sciences companies. This business helps customers reduce

---

[8] *UnitedHealth Group Incorporated (UNH)*, YAHOO! FINANCE, https://finance.yahoo.com/quote/UNH/profile (last visited Mar. 1, 2024).

[9] *Optum: Technology and data-enabled care delivery*, UNITEDHEALTH GROUP, https://www.unitedhealthgroup.com/people-and-businesses/businesses/optum.html (last visited Mar. 1, 2024).

[10] *Id*.

administrative costs, meet compliance mandates, improve clinical performance and transform operations."[11]

20. Optum Rx "offers a full spectrum of pharmacy care services that are making drugs more affordable and creating a better experience for consumers, filling more than 1.5 billion adjusted retail, mail and specialty drug prescriptions annually. Optum Rx solutions are rooted in evidence-based clinical guidelines."[12] In the regular course of its business, Optum Rx receives and maintains payment and health information from both patients and benefit sponsors.[13]

21. Change Healthcare is a healthcare technology company that provides data-driven and analytics-driven solutions for clinical, financial, administrative, and patient management to healthcare providers.[14] It holds itself out as providing "data and analytics, plus patient engagement and collaboration tools" to "providers and payers [to] optimize workflows, access the right information at the right time, and support the safest and most clinically appropriate care."[15] Change is one of the largest processors of prescription

---

[11] *Id*.

[12] *Id*.

[13] *Id*.

[14] *OptumInsight and Change Healthcare Combine to Advance a More Modern, Information and Technology-Enabled Health Care Platform*, OPTUM (Jan. 6, 2021), https://www.optum.com/en/about-us/news/page.hub.optuminsight-change-healthcare-combine.html.

[15] *The Change Healthcare Platform*, CHANGE HEALTHCARE, https://www.changehealthcare.com/platform (last visited Mar. 1, 2024).

medications in the United States and handles billing for more than 67,000 pharmacies across the country through which it handles 15 billion healthcare transactions annually.[16]

22. In October 2022, UHG completed its acquisition of Change Healthcare,[17] for it to merge with OptumInsight.[18] Optum described the purpose of the acquisition as follows:

> This combination unites two technology and service companies focused on serving health care. Their combined capabilities will more effectively connect and simplify core clinical, administrative and payment processes - resulting in better health outcomes and experiences for everyone, at lower cost. Change Healthcare brings key technologies, connections and advanced clinical decision, administrative and financial support capabilities, enabling better workflow and transactional connectivity across the health care system. Optum brings modern analytics, comprehensive clinical expertise, innovative technologies and extensive experience in improving operational and clinical performance.[19]

23. The President of UHG and CEO of Optum said that the combination of Change's and Optum's services "will help streamline and inform the vital clinical, administrative and payment processes on which health care providers and payers depend to serve patients."[20]

---

[16] Zack Whittaker, *UnitedHealth confirms ransomware gang behind Change Healthcare hack amid ongoing pharmacy outages*, TECHCRUNCH (Feb. 29, 2024, 9:15 AM) https://techcrunch.com/2024/02/29/unitedhealth-change-healthcare-ransomware-alphv-blackcat-pharmacy-outages/.

[17] *UnitedHealth Group Form 10-K (Dec.31, 2022),* SEC, https://www.sec.gov/ixviewer/ix.html?doc=/Archives/edgar/data/0000731766/000073176623000008/unh-20221231.htm (last visited Mar. 1, 2024).

[18] *OptumInsight and Change Healthcare Combine to Advance a More Modern, Information and Technology-Enabled Health Care Platform*, OPTUM (Jan. 6, 2021), https://www.optum.com/en/about-us/news/page.hub.optuminsight-change-healthcare-combine.html.

[19] Id.

[20] *Id*.

24. Thus, in the regular course of Optum's and Change's business, they receive and/or maintain patients' payment and health insurance information, as well as their sensitive health information.

25. As stated in UHG's latest annual report filed with the SEC, UHG "acquired all of the outstanding common shares of Change Healthcare"[21] such that Change Healthcare—like Optum—is now fully owned by UHG and operated as one of UHG's business segments.[22]

26. UnitedHealth Group Incorporated is responsible for overseeing Defendants' cybersecurity practices and procedures.

UHG's Privacy Practices

27. In the regular course of business, UHG stores patients' highly sensitive health information collected from a myriad of clients like Medicare, pharmacies, healthcare providers, and so on. This includes patients' full names, phone numbers, addresses, Social Security numbers, emails, medical records, dental records, payment information, claims information, insurance records, and much more.

28. Given the amount and sensitive nature of the data they store, Defendants maintain privacy policies describing how confidential and personal information is used and

---

[21] *UnitedHealth Group Form 10-K (Dec.31, 2022),* SEC, https://www.sec.gov/ixviewer/ix.html?doc=/Archives/edgar/data/0000731766/000073176623000008/unh-20221231.htm (last visited Mar. 1, 2024).

[22] *OptumInsight and Change Healthcare Combine to Advance a More Modern, Information and Technology-Enabled Health Care Platform*, OPTUM (Jan. 6, 2021), https://www.optum.com/en/about-us/news/page.hub.optuminsight-change-healthcare-combine.html.

disclosed. UnitedHealth Group Incorporated, UnitedHealthcare, and Optum operate under the same "Privacy Policy." They represent that they maintain "administrative, technical, and physical safeguards" designed to protect patients' information.[23] Their "Social Security Number Protection Policy" explicitly states that "[i]t is [their] policy to protect the confidentiality of Social Security numbers . . . that [they] receive or collect in the course of business. . . . It is [their] policy to limit access to SSNs to that which is lawful and to prohibit unlawful disclosure of SSNs."[24] Change Healthcare further represents that "[w]e implement and maintain organizational, technical, and administrative security measures designed to safeguard the data we process against unauthorized access, destruction, loss, alteration, or misuse. These measures are aimed at providing on-going integrity and confidentiality of data, including your personal information."[25]

29. Given its representations and experience handling highly sensitive PHI, UHG understood the need to protect patients' PHI and prioritize data security.

The Data Breach

---

[23] *Protecting Your Information*, UNITEDHEALTH GROUP, https://www.unitedhealthgroup.com/privacy.html#protectingyourinformation (last visited Mar. 1, 2024); *Protecting Your Information*, UNITEDHEALTHCARE, https://www.uhc.com/privacy#protectinginfo (last visited Mar. 1, 2024); *Protecting Your Information*, OPTUM, https://www.optum.com/en/privacy-policy.html#protect (last visited Mar. 1, 2024).

[24] *Social Security Number Protection Policy*, UNITEDHEALTH GROUP, https://www.unitedhealthgroup.com/privacy.html#socialsecurityprotection (last visited Mar. 1, 2024); *Social Security Number Protection Policy*, UNITEDHEALTCARE, https://www.uhc.com/privacy#ssprotection (last visited Mar. 1, 2024); *Social Security Number Protection Policy*, OPTUM, https://www.optum.com/en/privacy-policy.html#ssn (last visited Mar. 1, 2024).

[25] *Privacy Notice*, CHANGE HEALTHCARE, https://www.changehealthcare.com/privacy-notice (last visited Mar. 1, 2024).

30. On February 21, 2024, in an SEC filing, UnitedHealth Group Incorporated announced that "a suspected nation-state associated cyber security thread actor had gained access to some of the Change Healthcare information technology systems."[26] After detecting the breach, UnitedHealth Group Incorporated claimed to have "proactively isolated the impacted systems from other connecting systems…"[27] UnitedHealth Group Incorporated also said it was "working with law enforcement" and allegedly "notified customers, clients and certain government agencies" of the breach.[28] UnitedHealth Group Incorporated disclosed that the "network interruption [was] specific to Change Healthcare…"[29]

31. However, a week later Blackcat let the cat out of the bag. According to Blackcat, "[o]nly after threatening[sic] [UHG] to announce it was [Blackcat]" did UHG start telling a different story. Blackcat exposed the scope of the breach related to all Defendants. The group also revealed that it was "able to exfiltrate to be exact more than 6 TB of highly selective data" that "relates to all Change Health clients that have sensitive data being processed by the company." Blackcat identified several entities about whom it obtained sensitive data, including Medicare, Tricare, CVS-CareMark, Loomis, MetLife, and others.

---

[26] *UnitedHealth Group Incorporation Form 8-K*, SEC (Feb. 21, 2024), https://www.sec.gov/Archives/edgar/data/731766/000073176624000045/unh-20240221.htm.
[27] Id.
[28] Id.
[29] Id.

32. Blackcat disclosed that the exfiltrated data includes millions of: "active US military/navy personnel PII," "medical records," "dental records," "payments information," "Claims information," "Patients PII including Phone numbers/addresses/SSN/emails/etc…," "3000+ source code files for Change Health solutions…," "Insurance records," and "many many more." Blackcat warned UHG that "you are walking on a very thin line be careful you just might fall over."

33. Given that Change Healthcare handles 15 billion healthcare transactions (or about one-in-three U.S. patient records), the potential impact of the Data Breach is enormous and its effects may be felt for years to come.

The Data Breach was Preventable

34. UHG's cybersecurity practices and policies were inadequate and fell short of the industry-standard measures that should have been implemented long before the Data Breach occurred. This is especially true given that the healthcare industry is frequently one of the most targeted sectors for cyberattacks. Attacks using stolen credentials have increased precipitously over the last several years.

35. Healthcare providers and their affiliates like UHG are prime targets because of the information they collect and store, including financial information of patients, login credentials, insurance information, medical records and diagnoses, and personal information of employees and patients—all extremely valuable on underground markets.

36. This was known and obvious to UHG as it observed frequent public announcements of data breaches affecting healthcare providers and knew that information

of the type it collected, maintained, and stored is highly coveted and a frequent target of hackers.

37. It is well known that use of stolen credentials through long been the most popular and effective method of gaining authorized access to a company's internal networks and that companies should activate defenses to prevent such attacks.

38. According to the Federal Bureau of Investigation (FBI), phishing schemes designed to induce individuals to reveal personal information, such as network passwords, were the most common type of cybercrime in 2020, with such incidents nearly doubling in frequency between 2019 and 2020.[30] According to Verizon's 2021 Data Breach Investigations Report, 43% of breaches stemmed from phishing and/or pretexting schemes.[31]

39. The risk is so prevalent for healthcare providers that on October 28, 2020, the FBI and two federal agencies issued a "Joint Cybersecurity Advisory" warning that they have "credible information of an increased and imminent cybercrime threat to U.S. hospitals and healthcare providers."[32] The Cybersecurity and Infrastructure Security Agency (CISA), the Department of Health and Human Services (HHS), and the FBI issued

---

[30] *2020 Internet Crime Report*, FBI, https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf (last visited Mar. 1, 2024).

[31] *2021 DBIR Master's Guide*, VERIZON, https://www.verizon.com/business/resources/reports/dbir/2021/masters-guide/ (subscription required) (last visited Mar. 1, 2024).

[32] *Ransomware Activity Targeting the Healthcare and Public Health Sector*, JOINT CYBERSECURITY ADVISORY, https://us-cert.cisa.gov/sites/default/files/publications/AA20-302A_Ransomware%20_Activity_Targeting_the_Healthcare_and_Public_Health_Sector.pdf (last visited Mar. 1, 2024).

the advisory to warn healthcare providers to take "timely and reasonable precautions to protect their networks from these threats."[33]

40. There are two primary ways to mitigate the risk of stolen credentials: user education and technical security barriers. User education is the process of making employees or other users of a network aware of common disclosure schemes and implementing company-wide policies requiring the request or transfer of sensitive personal or financial information only through secure sources to known recipients.

41. Through technical security barriers, companies can also greatly reduce the flow of fraudulent e-mails by installing software that scans all incoming messages for harmful attachments or malicious content and implementing certain security measures governing e-mail transmissions, including Sender Policy Framework (SPF) (e-mail authentication method used to prevent spammers from sending messages on behalf of a company's domain), DomainKeys Identified Mail (DKIM) (e-mail authentication method used to ensure messages are not altered in transit between the sending and recipient servers), and Domain-based Message Authentication, Reporting and Conformance (DMARC), which "builds on the widely deployed [SPF] and [DKIM] protocols, adding a reporting function that allows senders and receivers to improve and monitor protection of the domain from fraudulent email."[34]

42. In addition to mitigating the risk of stolen credentials, the CISA guidance encourages organizations to prevent unauthorized access by:

---

[33] Id.

[34] Id.

- Conducting regular vulnerability scanning to identify and address vulnerabilities, particularly on internet-facing devices;
- Regularly patching and updating software to latest available versions, prioritizing timely patching of internet-facing servers and software processing internet data;
- Ensuring devices are properly configured and that security features are enabled;
- Employing best practices for use of Remote Desktop Protocol (RDP) as threat actors often gain initial access to a network through exposed and poorly secured remote services; and
- Disabling operating system network file sharing protocol known as Server Message Block (SMB) which is used by threat actors to travel through a network to spread malware or access sensitive data.[35]

43. The CISA guidance further recommends use of a centrally managed antivirus software utilizing automatic updates that will protect all devices connected to a network (as opposed to requiring separate software on each individual device), as well as implementing a real-time intrusion detection system that will detect potentially malicious network activity that occurs prior to ransomware deployment.[36]

44. Despite holding the PHI of millions of patients, UHG failed to adhere these recommended best practices. Indeed, had UHG implemented common sense security measures like network segmentation and POLP, the hackers never could have accessed millions of patient files and the breach would have been prevented or much smaller in

[35] CISA Guide at 4.
[36] *Id.* at 5.

scope. UHG also lacked the necessary safeguards to detect and prevent phishing attacks and failed to implement adequate monitoring or control systems to detect the unauthorized infiltration after it occurred.

45. UHG, like any entity in the healthcare industry its size storing valuable data, should have had robust protections in place to detect and terminate a successful intrusion long before access and exfiltration could expand to millions of patient files. UHG's below-industry-standard procedures and policies are inexcusable given its knowledge that it was a prime target for cyberattacks.

Allegations Relating to Plaintiff Nicolas Keriazis

46. Plaintiff Nicolas Keriazis lives and resides in Riverside, California and uses CVS Pharmacy to fill his medical prescriptions.

47. For purposes of receiving medical treatment, Mr. Keriazis was required to provide his healthcare provider with his sensitive personal information, including, among other information, his full name, contact information, date of birth, Social Security number, and health insurance information.

48. Mr. Keriazis's healthcare provider also maintained his patient account numbers, health insurance information, medical record numbers, dates of service, provider names, and medical and clinical treatment information.

49. Mr. Keriazis's healthcare provider shared his PHI with CVS Pharmacy who then shared it with UHG in connection with filling Mr. Keriazis's prescription. UHG stored Mr. Keriazis's PHI in its systems.

50. Mr. Keriazis learned of the Data Breach after having challenges filling his prescription. Sometime after February 21, 2024, Mr. Keriazis went to fill his prescription at his local CVS Pharmacy but was unsuccessful. As a result of the Data Breach, Mr. Keriazis could not timely fill his prescription for his medication subjecting him to potential negative health risks.

51. Furthermore, because the Data Breach impacted PHI of patients associated with CVS Pharmacy, Mr. Keriazis has also spent time and effort researching the breach and reviewing his financial and medical account statements for evidence of unauthorized activity, which he will continue to do indefinitely. In addition to the ramifications associated with not being able to timely access necessary medications, Mr. Keriazis also suffered emotional distress knowing that his highly personal medical and treatment information is no longer confidential and can be used for blackmail, extortion, medical-related identity theft or fraud, and any number of additional harms against him for the rest of his life.

UHG Failed to Comply with Federal Law and Regulatory Guidance

52. UHG is covered by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") (see 45 C.F.R. § 160.102) and as such is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

53. These rules establish national standards for the protection of patient information, including PHI, defined as "individually identifiable health information" which either "identifies the individual" or where there is a "reasonable basis to believe the information can be used to identify the individual," that is held or transmitted by a healthcare provider. 45 C.F.R. § 160.103.

54. HIPAA limits the permissible uses of "protected health information" and prohibits unauthorized disclosures of "protected health information."[37]

55. HIPAA requires that UHG implement appropriate safeguards for this information.[38]

56. HIPAA requires that UHG provide notice of a breach of unsecured protected health information, which includes protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons—i.e. non-encrypted data.[39]

57. Despite these requirements, UHG failed to comply with its duties under HIPAA and its own privacy policies. Indeed, UHG failed to:

a. Maintain an adequate data security system to reduce the risk of data breaches and cyberattacks;

b. Adequately protect the PHI of patients;

---

[37] 45 C.F.R. § 164.502.
[38] 45 C.F.R. § 164.530(c)(1).
[39] 45 C.F.R. § 164.404; 45 C.F.R. § 164.402.

c. Ensure the confidentiality and integrity of electronically protected health information created, received, maintained, or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

d. Implement technical policies and procedures for electronic information systems that maintain electronically protected health information to allow access only to those persons or software programs that have been granted access rights, in violation of 45 C.F.R. § 164.312(a)(1);

e. Implement adequate policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 C.F.R. § 164.308(a)(1)(i);

f. Implement adequate procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

g. Protect against reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 C.F.R. § 164.306(a)(3);

h. Ensure compliance with the electronically protected health information security standard rules by their workforces, in violation of 45 C.F.R. § 164.306(a)(4); and/or

i. Train all members of their workforces effectively on the policies and procedures with respect to protected health information as necessary and appropriate for the members of their workforces to carry out their functions

and to maintain security of protected health information, in violation of 45 C.F.R. § 164.530(b).

58. Additionally, federal agencies have issued recommendations and guidelines to help minimize the risks of a data breach for businesses holding sensitive data. For example, the Federal Trade Commission ("FTC") has issued numerous guides for business highlighting the importance of reasonable data security practices, which should be factored into all business-related decision making.[40]

59. The FTC's publication *Protecting Personal Information: A Guide for Business* sets forth fundamental data security principles and practices for businesses to implement and follow as a means to protect sensitive data.[41] Among other things, the guidelines note that businesses should (a) protect the personal customer information that they collect and store; (b) properly dispose of personal information that is no longer needed; (c) encrypt information stored on their computer networks; (d) understand their network's vulnerabilities; and (e) implement policies to correct security problems. The FTC guidelines further recommend that businesses use an intrusion detection system, monitor all incoming traffic for unusual activity, monitor for large amounts of data being transmitted from their system, and have a response plan ready in the event of a breach.[42]

---

[40] *Start with Security*, FTC, https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited Mar. 1, 2024).

[41] *Protecting Personal Information*, FTC, https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Mar. 1, 2024).

[42] *Id*.

60. Additionally, the FTC recommends that companies limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security; monitor for suspicious activity on the network, and verify that third-party service providers have implemented reasonable security measures.[43] This is consistent with guidance provided by the FBI, HHS, and the principles set forth in the CISA 2020 guidance.

61. The FTC has brought enforcement actions against businesses for failing to reasonably protect customer information, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.[44]

62. UHG was fully aware of its obligation to implement and use reasonable measures to protect the PHI of the patients but failed to comply with these basic recommendations and guidelines that would have prevented this breach from occurring. UHG's failure to employ reasonable measures to protect against unauthorized access to patient information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

---

[43] Start With Security, supra note 41.

[44] *Privacy and Security Enforcement*, FTC, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement (last visited Mar. 1, 2024).

The Impact of the Data Breach on Victims

63. The PHI exposed in the Data Breach is highly coveted and valuable on underground markets as it can be used to commit identity fraud, including medical-related identity theft and fraud, one of the most dangerous and costly forms of identity theft.

64. According to a *Reuters* investigation that included interviews with nearly a dozen healthcare executives, cybersecurity investigators, and fraud experts, medical data for sale on underground markets "includes names, birth dates, policy numbers, diagnosis codes and billing information" which fraudsters commonly use "to create fake IDs to buy medical equipment or drugs that can be resold, or they combine a patient number with a false provider number and file made-up claims with insurers."[45]

65. According to Tom Kellermann, chief cybersecurity officer of cybersecurity firm Carbon Black, "Health information is a treasure trove for criminals [because] by compromising it, by stealing it, by having it sold, you have seven to 10 personal identifying characteristics of an individual."[46] For this reason, a patient's full medical records can sell for up to $1,000 on the dark web, while credit card numbers and Social Security numbers may cost $5 or less.[47]

---

[45] Caroline Humer & Jim Finkle, *Your medical record is worth more to hackers than your credit card*, REUTERS (Sep. 24, 2014, 1:44 PM), .https://www.reuters.com/article/us-cybersecurity-hospitals/your-medical-recordis-worth-more-to-hackers-than-your-credit-card-idUSKCN0HJ21I20140924.

[46] Andrew Steger, *What Happens to Stolen Healthcare Data?*, HEALTHTECH (Oct. 30, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon .

[47] Brian Stack, *Here's How Much Your Personal Information Is Selling for on the Dark Web*, EXPERIAN (Dec. 6, 2017), https://www.experian.com/blogs/ask-experian/heres-how-much-your-personalinformation-is-selling-for-on-the-dark-web/.

66. As noted by Paul Nadrag, a software developer for medical device integration and data technology company Capsule Technologies: "The reason for this price discrepancy—like any other good or service—is perceived value. While a credit card number is easily canceled, medical records contain a treasure trove of unalterable data points, such as a patient's medical and behavioral health history and demographics, as well as their health insurance and contact information. Once records are stolen, cybercriminals often tap into members of a criminal network on the dark web experienced in drug trafficking and money laundering who are eager to buy medical records to support their criminal activities, such as illegally obtaining prescription medications, filing bogus medical claims or simply stealing the patient's identity to open credit cards and fraudulent loans."[48]

67. Indeed, while federal law generally limits an individual's responsibility for fraudulent charges on a credit card to $50, there are no such protections for a stolen medical identity. According to a 2015 survey on medical identity theft conducted by the Ponemon Institute, victims of medical identity theft spent an average of $13,500 in out-of-pocket costs to resolve the crime.[49] Frequently, this information was used to obtain medical services or treatments (59%), obtain prescription drugs (56%), or receive Medicare and

---

[48] Paul Nadrag, *Industry Voices—Forget credit card numbers. Medical records are the hottest items on the dark web*, FIERCE HEALTHCARE (Jan. 26, 2021, 3:55 PM), https://www.fiercehealthcare.com/hospitals/industry-voices-forget-credit-card-numbers-medicalrecords-are-hottest-items-dark-web.

[49] *Fifth Annual Study on Medical Identity Theft*, PONEMON INSTITUTE (Feb. 2015), https://static.nationwide.com/static/2014_Medical_ID_Theft_Study.pdf?r=65 ("Ponemon Study").

Medicaid benefits (52%). Only 14% of respondents said that the identity thieves used the information to obtain fraudulent credit accounts, indicating that medical information is a much more profitable market.[50]

68. According to the Ponemon study, "[t]hose who have resolved the crime spent, on average, more than 200 hours on such activities as working with their insurer or healthcare provider to make sure their personal medical credentials are secured and can no longer be used by an imposter and verifying their personal health information, medical invoices and claims and electronic health records are accurate."[51]

69. Additionally, the study found that medical identity theft can have a negative impact on reputation as 45% of respondents said that medical identity theft affected their reputation mainly because of embarrassment due to disclosure of sensitive personal health conditions, with 19% responding that they missed out on employment opportunities as a result.[52]

70. Exacerbating the problem, victims of medical identity theft oftentimes struggle to resolve the issue because HIPAA regulations require the victim to be personally involved in the resolution of the crime.[53] In some cases, victims may not even be able to access medical records using their personal information because they include a false name or data points taken from another person's records. Consequently, only 10% of medical

[50] *Id*. at 9.
[51] *Id*. at 2.
[52] *Id*. at 14.
[53] *Id*. at 1.

identity theft victims responded that they "achiev[ed] a completely satisfactory conclusion of the incident."[54]

71. Moreover, it can take months or years for victims to even discover they are the victim of medical-related identity theft or fraud given the difficulties associated with accessing medical records and healthcare statements. For example, the FTC notes that victims may only discover their identity has been compromised after they:

- Receive a bill for medical services they did not receive;
- Get contacted by a debt collector about medical debt they do not owe;
- See medical collection notices on their credit report that they do not recognize;
- Find erroneous listings of office visits or treatments on their explanation of benefits (EOB);
- Receive information from their health plan that they have reached their limit on benefits; or
- Be denied insurance because their medical records show a condition they do not have.[55]

72. Perhaps most dangerous, however, is the potential for misdiagnoses or treatment. According to Ann Patterson, a senior vice president of the Medical Identity Fraud Alliance, "About 20 percent of victims have told us that they got the wrong diagnosis

---

[54] *Id*.

[55] *Medical Identity Theft, FAQs for Health Care Providers and Health Plans*, FTC.GOV, https://www.ftc.gov/system/files/documents/plain-language/bus75-medical-identity-theft-faqhealth-care-health-plan.pdf (last visited Mar. 1, 2024).

or treatment, or that their care was delayed because there was confusion about what was true in their records due to the identity theft." [56] This echoes the Ponemon study, which notes that "many respondents are at risk for further theft or errors in healthcare records that could jeopardize medical treatments and diagnosis."[57]

73. According to a Consumer Reports article entitled *The Rise of Medical Identity Theft*, this outcome "isn't a hypothetical problem" as the "long tail on medical identity theft can create havoc in victims' lives."[58] As one example, a pregnant woman reportedly used a victim's medical identity to pay for maternity care at a nearby hospital. When the infant was born with drugs in her system, the state threatened to take the *victim's* four children away—not realizing her identity had been stolen. The victim ultimately had to submit to a DNA test to remove her name from the infant's birth certificate, but it took years to get her medical records corrected.[59]

74. Other types of medical fraud include "leveraging details specific to a disease or terminal illness, and long-term identity theft."[60] According to Tom Kellermann, "Traditional criminals understand the power of coercion and extortion. By having healthcare information—specifically, regarding a sexually transmitted disease or terminal

---

[56] Michelle Andrews, *The Rise of Medical Identity Theft*, CONSUMER REPORTS, https://www.consumerreports.org/medical-identity-theft/medical-identity-theft/ (last visited Mar. 1, 2024).

[57] Ponemon Study at 1.

[58] Michelle Andrews, *The Rise of Medical Identity Theft*, CONSUMER REPORTS, https://www.consumerreports.org/medical-identity-theft/medical-identity-theft/ (last visited Mar. 1, 2024).

[59] *Id*.

[60] Andrew Steger, *What Happens to Stolen Healthcare Data?*, HEALTHTECH (Oct. 30, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon.

illness—that information can be used to extort or coerce someone to do what you want them to do."[61] Long-term identity theft occurs when fraudsters combine a victim's data points, including publicly-available information or data points exposed in other data breaches, to create new identities, open false lines of credit, or commit tax fraud that can take years to remedy.

75. Many victims of the Data Breach have likely already experienced significant harms as the result of the Data Breach, including, but not limited to, medical-related identity theft and fraud. Plaintiffs and class members have also spent time, money, and effort dealing with the fallout of the Data Breach, including purchasing credit monitoring services, reviewing financial and healthcare statements, checking credit reports, and spending time and effort searching for unauthorized activity.

76. It is no wonder then that identity theft exacts a severe emotional toll on its victims. The 2017 Identity Theft Resource Center survey evidences the emotional suffering experienced by victims of identity theft:

- 75% of respondents reported feeling severely distressed;
- 67% reported anxiety;
- 66% reported feelings of fear related to personal financial safety;
- 37% reported fearing for the financial safety of family members;
- 24% reported fear for their physical safety;

[61] *Id*.

- 15.2% reported a relationship ended or was severely and negatively impacted by the identity theft; and
- 7% reported feeling suicidal.[62]

77. Identity theft can also exact a physical toll on its victims. The same survey reported that respondents experienced physical symptoms stemming from their experience with identity theft:

- 48.3% of respondents reported sleep disturbances;
- 37.1% reported an inability to concentrate / lack of focus;
- 28.7% reported they were unable to go to work because of physical symptoms;
- 23.1% reported new physical illnesses (aches and pains, heart palpitations, sweating, stomach issues); and
- 12.6% reported a start or relapse into unhealthy or addictive behaviors.[63]

78. The unauthorized disclosure of the sensitive PHI to data thieves also reduces its inherent value to its owner, which has been recognized by courts as an independent form of harm.[64]

---

[62] *Identity Theft: The Aftermath 2017*, ITRC, https://www.idtheftcenter.org/wpcontent/uploads/images/page-docs/Aftermath_2017.pdf (last visited Jan. 17, 2024).

[63] *Id.*

[64] *See In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig.*, 440 F. Supp. 3d 447, 462 (D. Md. 2020) ("Neither should the Court ignore what common sense compels it to acknowledge—the value that personal identifying information has in our increasingly digital economy. Many companies, like Marriott, collect personal information. Consumers too recognize the value of their personal information and offer it in exchange for goods and services.").

79. Consumers are injured every time their data is stolen and traded on underground markets, even if they have been victims of previous data breaches. Indeed, the dark web is comprised of multiple discrete repositories of stolen information that can be aggregated together or accessed by different criminal actors who intend to use it for different fraudulent purposes. Each data breach increases the likelihood that a victim's personal information will be exposed to more individuals who are seeking to misuse it at the victim's expense.

80. As the result of the wide variety of injuries that can be traced to the Data Breach, Plaintiff and class members have and will continue to suffer economic loss and other actual harm for which they are entitled to damages, including, but not limited to, the following:

a. the unconsented disclosure of confidential information to a third party;

b. losing the value of the explicit and implicit promises of data security;

c. identity theft and fraud resulting from the theft of their PHI;

d. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

e. anxiety, emotional distress, and loss of privacy;

f. costs associated with purchasing credit monitoring, credit freezes, and identity theft protection services;

g. unauthorized charges and loss of use of and access to their financial and investment account funds and costs associated with inability to obtain money from their accounts or being limited in the amount of money they were

permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit;

h. lowered credit scores resulting from credit inquiries following fraudulent activities;

i. costs associated with time spent and the loss of productivity or the enjoyment of one's life from taking time to address and attempt to mitigate and address the actual and future consequences of the Data Breach, including searching for fraudulent activity, imposing withdrawal and purchase limits on compromised accounts, and the stress, nuisance, and annoyance of dealing with the repercussions of the Data Breach; and

j. the continued, imminent, and certainly impending injury flowing from potential fraud and identify theft posed by their PHI being in the possession of one or many unauthorized third parties.

81. Even in instances where an individual is reimbursed for a financial loss due to identity theft or fraud, that does not make that individual whole again as there is typically significant time and effort associated with seeking reimbursement.

82. There may also be a significant time lag between when personal information is stolen and when it is misused for fraudulent purposes. According to the Government Accountability Office, which conducted a study regarding data breaches: "law enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that

attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm."[65]

83. Plaintiff and class members place significant value in data security. According to a survey conducted by cyber-security company FireEye Mandiant, approximately 50% of consumers consider data security to be a main or important consideration when making purchasing decisions and nearly the same percentage would be willing to pay more in order to work with a provider that has better data security. Likewise, 70% of consumers would provide less personal information to organizations that suffered a data breach.[66]

84. Because of the value consumers place on data privacy and security, healthcare providers with robust data security practices are viewed more favorably by patients and can command higher prices than those who do not. Consequently, had patients known the truth about UHG's data security practices—that it did not adequately protect and store their PHI —they would not have sought medical care and/or filled prescriptions practices affiliated with UHG or would have paid significantly less. As such, Plaintiff and Class members did not receive the benefit of their bargain with UHG because they paid for the value of services they did not receive.

---

[65] PERSONAL INFORMATION: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent is Unknown, GAO, http://www.gao.gov/new.items/d07737.pdf (last visited Mar. 1, 2024).

[66] *BEYOND THE BOTTOM LINE: THE REAL COST OF DATA BREACHES*, FIREEYE, https://www2.fireeye.com/rs/848-DID-242/images/rpt-beyond-bottomline.pdf (last visited Mar. 1, 2024).

85. Plaintiff and Class members have a direct interest in UHG's promises and duties to protect their PHI, *i.e.*, that UHG *not increase* their risk of identity theft and fraud. Because UHG failed to live up to its promises and duties in this respect, Plaintiff and Class members seek the present value of identity protection services to compensate them for the present harm and present and continuing increased risk of harm caused by UHG wrongful conduct. Through this remedy, Plaintiff and Class members seek to restore themselves and class members as close to the same position as they would have occupied but for UHG's wrongful conduct, namely its failure to adequately protect Plaintiff's and Class members' PHI.

86. Plaintiff and Class members further seek to recover the value of the unauthorized access to their PHI permitted through UHG's wrongful conduct. This measure of damages is analogous to the remedies for unauthorized use of intellectual property. Like a technology covered by a trade secret or patent, use or access to a person's PHI is non-rivalrous—the unauthorized use by another does not diminish the rights-holder's ability to practice the patented invention or use the trade-secret protected technology. Nevertheless, a plaintiff may generally recover the reasonable use value of the IP—*i.e.*, a "reasonable royalty" from an infringer. This is true even though the infringer's use did not interfere with the owner's own use (as in the case of a non-practicing patentee) and even though the owner would not have otherwise licensed such IP to the infringer. A similar royalty or license measure of damages is appropriate here under common law damages principles authorizing recovery of rental or use value. This measure is appropriate because (a) Plaintiffs and class members have a protectible property interest in their PHI;

(b) the minimum damages measure for the unauthorized use of personal property is its rental value; and (c) rental value is established with reference to market value, *i.e.*, evidence regarding the value of similar transactions.

87. Because UHG continues to hold the PHI of patients, Plaintiff and Class members have an interest in ensuring that their PHI is secured and not subject to further theft.

CLASS ACTION ALLEGATIONS

88. Plaintiff seeks relief in his individual capacity and as a representative of all others who are similarly situated. Pursuant to Federal Rule of Civil Procedure 23, Plaintiff brings this action on behalf of himself and the Class defined as: All individuals whose personal health information was compromised in the Data Breach announced by UnitedHealth Group Incorporated in February 2024 (the "Class").

89. Specifically excluded from the Class are Defendant; its officers, directors, or employees; any entity in which Defendant has a controlling interest; and any affiliate, legal representative, heir, or assign of Defendant. Also excluded from the Class are any federal, state, or local governmental entities, any judicial officer presiding over this action and the members of their immediate family and judicial staff, and any juror assigned to this action.

90. Class Identity: The members of the Class are readily identifiable and ascertainable. UHG and/or its affiliates, among others, possess the information to identify and contact class members.

91. Numerosity: The members of the Class are so numerous that joinder of all of them is impracticable. Blackcat revealed that the PHI of millions of patients associated with UHG is compromised.

92. Typicality: Plaintiff's claims are typical of the claims of the members of the Class because all class members had their PHI compromised in the Data Breach and were harmed as a result.

93. Adequacy: Plaintiff will fairly and adequately protect the interests of the Class. Plaintiff has no known interest antagonistic to those of the Class and his interests are aligned with Class members' interests. Plaintiff was subject to the same Data Breach as class members, suffered similar harms, and face similar threats due to the Data Breach. Plaintiff has also retained competent counsel with significant experience litigating complex class actions, including data breach cases involving multiple classes and data breach claims.

94. Commonality and Predominance: There are questions of law and fact common to the Class such that there is a well-defined community of interest in this litigation. These common questions predominate over any questions affecting only individual class members. The common questions of law and fact include, without limitation:

a. Whether UHG owed Plaintiff and class members a duty to implement and maintain reasonable security procedures and practices to protect their PHI;

b. Whether UHG received a benefit without proper restitution making it unjust for UHG to retain the benefit without commensurate compensation;

c. Whether UHG acted negligently in connection with the monitoring and/or protection of Plaintiff's and class members' PHI;

d. Whether UHG violated its duty to implement reasonable security systems to protect Plaintiff's and class members' PHI;

e. Whether UHG's breach of its duty to implement reasonable security systems directly and/or proximately caused damages to Plaintiff and class members;

f. Whether UHG adequately addressed and fixed the vulnerabilities that enabled the Data Breach;

g. Whether UHG and class members are entitled to damages to pay for future protective measures like credit monitoring and monitoring for misuse of medical information; and

h. Whether class members are entitled to compensatory damages, punitive damages, and/or statutory or civil penalties as a result of the Data Breach.

95. UHG has engaged in a common course of conduct and Plaintiff and class members have been similarly impacted by UHG's failure to maintain reasonable security procedures and practices to protect patients' PHI.

96. Superiority: A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law

and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most if not all class members would find the cost of litigating their individual claims prohibitively high and have no effective remedy. The prosecution of separate actions by individual class members would create a risk of inconsistent or varying adjudications with respect to individual class members and risk inconsistent treatment of claims arising from the same set of facts and occurrences. Plaintiff knows of no difficulty likely to be encountered in the maintenance of this action as a class action under the applicable rules.

CLAIMS FOR RELIEF

COUNT I
Negligence
(On Behalf of Plaintiffs and the Class)

97. Plaintiff repeats and realleges every allegation set forth in the preceding paragraphs.

98. UHG required Plaintiff's and class members' PHI as a condition of receiving healthcare services and to perform UHG's insurer functions in connection with its patients received medical treatment. UHG stored the data for purposes of providing health insurance services as well as for commercial gain.

99. UHG owed Plaintiff and class members a duty to exercise reasonable care in protecting their PHI from unauthorized disclosure or access. UHG acknowledged this duty in its privacy polices, where it promised not to disclose PHI, including SSNs, without authorization and to abide by all federal laws and regulations.

100. UHG owed a duty of care to Plaintiff and class members to provide adequate data security, consistent with industry standards, to ensure that UHG's systems and networks adequately protected the PHI.

101. Under HIPAA, UHG had a special relationship with Plaintiff and class members who entrusted UHG to adequately safeguard their confidential personal, financial, and medical information.

102. Defendant's duty to use reasonable care in protecting PHI arises as a result of the parties' relationship, as well as common law and federal law, including the HIPAA regulations described above and UHG's own policies and promises regarding privacy and data security.

103. UHG knew, or should have known, of the risks inherent in collecting and storing PHI in a centralized location, UHG's vulnerability to network attacks, and the importance of adequate security.

104. UHG breached its duty to Plaintiff and class members in numerous ways, as described herein, including by:

- Failing to exercise reasonable care and implement adequate security systems, protocols, and practices sufficient to protect the PHI of Plaintiff and class members;
- Failing to comply with industry standard data security measures for the healthcare industry leading up to the Data Breach;
- Failing to comply with its own privacy policies;
- Failing to comply with regulations protecting the PHI at issue during the period of the Data Breach;

- Failing to adequately monitor, evaluate, and ensure the security of UHG's network and systems; and

- Failing to recognize in a timely manner that PHI had been compromised.

105. Plaintiff'' and class members' PHI would not have been compromised but for UHG's wrongful and negligent breach of its duties.

106. UHG's failure to take proper security measures to protect the sensitive PHI of Plaintiff and class members as described in this Complaint, created conditions conducive to a foreseeable, intentional criminal act, namely the unauthorized access and copying of PHI by unauthorized third parties. Given that healthcare providers and affiliates are prime targets for hackers, Plaintiff and class members are part of a foreseeable, discernible group that was at high risk of having their PHI misused or disclosed if not adequately protected by UHG.

107. It was also foreseeable that UHG's failure to provide timely and forthright notice of the Data Breach would result in injury to Plaintiff and class members.

108. As a direct and proximate result of UHG's conduct, Plaintiff and class members have and will suffer damages including: (i) the loss of rental or use value of their PHI; (ii) the unconsented disclosure of their PHI to unauthorized third parties; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, fraud, and/or unauthorized use of their PHI; (iv) lost opportunity costs associated with addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from fraud and identity theft; (v) time, effort, and expense associated

with placing fraud alerts or freezes on credit reports; (vi) anxiety, emotional distress, loss of privacy, and other economic and non-economic losses; (vii) the continued risk to their PHI, which remains in UHG's possession and is subject to further unauthorized disclosures so long as UHG fails to undertake appropriate and adequate measures to protect it; (viii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of compromised PHI for the rest of their lives; and (ix) any nominal damages that may be awarded.

COUNT II
Negligence *Per Se*
(On Behalf of Plaintiffs and the Class)

109. Plaintiff repeats and realleges every allegation set forth in the preceding paragraphs.

110. UHG is covered by HIPAA, 45 C.F.R. § 160.102, and is therefore obligated to comply with all rules and regulations under 45 C.F.R. Parts 160 and 164.

111. 45 C.F.R. Part 164 governs "Security and Privacy," with Subpart A providing "General Provisions," Subpart B regulating "Security Standards for the Protection of Electronic Protected Health Information," Subpart C providing requirements for "Notification in the Case of Breach of Unsecured Protected Health Information," and Subpart E governing "Privacy of Individually Identifiable Health Information."

112. 45 C.F.R. § 164.104 states that the "standards, requirements, and implementation specifications adopted under this part" apply to covered entities and their business associates, such as UHG.

113. UHG is obligated under HIPAA to, among other things, "ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits" and "protect against any reasonably anticipated threats or hazards to the security or integrity of such information." 45 C.F.R. § 164.306.

114. 45 C.F.R. Sections 164.308 (Administrative safeguards), 164.310 (Physical safeguards), 164.312 (Technical safeguards), 164.314 (Organizational requirements), and 164.316 (Policies and procedures and documentation requirements) provide mandatory standards that all covered entities must adhere to.

115. UHG violated HIPAA by failing to adhere to and meet the required standards as set forth in 45 C.F.R. §§ 164.308, 164.310, 164.312, 164.314, and 164.316.

116. HIPAA requires UHG to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). The confidential data at issue in this case constitutes "protected health information" within the meaning of HIPAA.

117. HIPAA further requires UHG to disclose the unauthorized access and theft of the PHI to Plaintiff and class members "without unreasonable delay" so that they can take appropriate measures to mitigate damages, protect against adverse consequences, and detect misuse of their PHI. See 45 C.F.R. § 164.404.

118. UHG violated HIPAA by failing to reasonably protect Plaintiff's and class members' PHI and by failing to give timely and complete notice, as described herein.

119. UHG's violations of HIPAA constitute negligence *per se*.

120. Plaintiff and class members are within the class of persons that HIPAA and its implementing regulations were intended to protect.

121. The harm that occurred as a result of the Data Breach is the type of harm HIPAA was intended to guard against.

122. Additionally, Section 5 of the Federal Trade Commission Act ("FTC Act") prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as UHG, of failing to use reasonable measures to protect PHI. 15 U.S.C. § 45(a)(1).

123. The FTC publications and orders described above also form part of the basis of UHG's duty in this regard.

124. UHG violated Section 5 of the FTC Act by failing to use reasonable measures to protect PHI and failing to comply with applicable industry standards. UHG's conduct was unreasonable given the nature and amount of PHI they obtained, stored, and disseminated in the regular course of their business, and the foreseeable consequences of a data breach, including, specifically, the significant damage that would result to Plaintiff and class members.

125. UHG's violations of Section 5 of the FTC Act constitute negligence *per se*.

126. Plaintiff and class members are within the class of persons that the FTC Act was intended to protect.

127. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against

businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and class members. As a direct and proximate result of UHG's negligence *per se*, Plaintiff and class members sustained actual losses and damages as alleged herein. Plaintiff and class members alternatively seek an award of nominal damages.

COUNT III
Breach of Third-Party Beneficiary Contract
(On Behalf of Plaintiffs and the Class)

128. Plaintiff repeats and realleges every allegation set forth in the preceding paragraphs.

129. Acting in the ordinary course of business, UHG contracts with several healthcare providers to provide healthcare insurance to patients. UHG obtains patients' PHI received from its healthcare providers to perform its insurance functions.

130. Upon information and belief, each of those respective contracts contained provisions requiring UHG to protect the patient information that UHG received in order to provide such insurance functions in carrying out the business of the contract.

131. Upon information and belief, these provisions requiring UHG acting in the ordinary course of business to protect the personal information of patients were intentionally included for the direct benefit of Plaintiff and class members, such that Plaintiff and class members are intended third party beneficiaries of these contracts, and therefore entitled to enforce them.

132. UHG breached these contracts while acting in the ordinary course of business by not protecting Plaintiff's and class member's personal information, as stated herein.

133. As a direct and proximate result of UHG's breaches, Plaintiff and class members sustained actual losses and damages described in detail herein. Plaintiff and class members alternatively seek an award of nominal damages.

COUNT IV
Unjust Enrichment
(On Behalf of Plaintiffs and the Class)

134. Plaintiff repeats and realleges every allegation set forth in the preceding paragraphs.

135. Plaintiff and class members have an interest, both equitable and legal, in their PHI that was conferred upon, collected by, and maintained by the UHG and which was stolen in the Data Breach. This information has independent value.

136. Plaintiff and class members conferred a monetary benefit on UHG in the form of payments for medical and healthcare services, including those paid indirectly by Plaintiff and class members to UHG.

137. UHG appreciated and had knowledge of the benefits conferred upon it by Plaintiff and class members.

138. The price for medical and healthcare services that Plaintiff and class members paid (directly or indirectly) to UHG should have been used by UHG, in part, to pay for the administrative costs of reasonable data privacy and security practices and procedures.

139. Likewise, in exchange for receiving Plaintiff's and class members' valuable PHI, which UHG was able to use for its own business purposes and which provided actual

value to UHG, UHG was obligated to devote sufficient resources to reasonable data privacy and security practices and procedures.

140. As a result of UHG's conduct, Plaintiff and class members suffered actual damages as described herein. Under principals of equity and good conscience, UHG should be compelled to disgorge into a common fund for the benefit of Plaintiff and class members all unlawful or inequitable proceeds they received from Plaintiff and class members, including damages equaling the difference in value between medical and healthcare services that included implementation of reasonable data privacy and security practices that Plaintiff and class members paid for and the services without reasonable data privacy and security practices that they actually received.

COUNT V
Declaratory Judgment
(On Behalf of Plaintiffs and the Class)

141. Plaintiff repeats and realleges every allegation set forth in the preceding paragraphs.

142. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq*., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal statutes described in this Complaint.

143. An actual controversy has arisen in the wake of the Data Breach regarding UHG's present and prospective common law and other duties to reasonably safeguard PHI and whether UHG is currently maintaining data security measures adequate to protect

Plaintiff and class members from further cyberattacks and data breaches that could compromise their PHI.

144. UHG still possesses PHI pertaining to Plaintiff and class members, which means their PHI remains at risk of further breaches because UHG's data security measures remain inadequate. Plaintiff and class members continue to suffer injuries as a result of the compromise of their PHI and remain at an imminent risk that additional compromises of their PHI will occur in the future.

145. Pursuant to the Declaratory Judgment Act, Plaintiff seeks a declaration that: (a) UHG's existing data security measures do not comply with its obligations and duties of care; and (b) in order to comply with their obligations and duties of care, (1) UHG must have policies and procedures in place to ensure the parties with whom it shares sensitive personal information maintain reasonable, industry-standard security measures, including, but not limited to, those listed at (ii), (a)-(i), *infra*, and must comply with those policies and procedures; (2) UHG must: (i) purge, delete, or destroy in a reasonably secure manner Plaintiff's and class members' PHI if it is no longer necessary to perform essential business functions so that it is not subject to further theft; and (ii) implement and maintain reasonable, industry-standard security measures, including, but not limited to:

a. Engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on UHG's systems on a periodic basis, and ordering UHG to promptly correct any problems or issues detected by such third-party security auditors;

b. Engaging third-party security auditors and internal personnel to run automated security monitoring;

c. Auditing, testing, and training its security personnel regarding any new or modified procedures;

d. Encrypting PHI and segmenting PHI by, among other things, creating firewalls and access controls so that if one area of UHG's systems is compromised, hackers cannot gain access to other portions of its systems;

e. Purging, deleting, and destroying in a reasonable and secure manner PHI not necessary to perform essential business functions;

f. Conducting regular database scanning and security checks;

g. Conducting regular employee education regarding best security practices;

h. Implementing multi-factor authentication and POLP to combat system-wide cyberattacks; and

i. Routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach.

REQUEST FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and the Class set forth herein, respectfully requests the following relief:

A. That the Court certify this action as a class action pursuant to Rule 23 of the Federal Rules of Civil Procedure, appoint Plaintiff as class representatives and Plaintiff's counsel as Class Counsel;

B. That the Court grant permanent injunctive relief to prohibit and prevent UHG from continuing to engage in the unlawful acts, omissions, and practices described herein;

C. That the Court award Plaintiff and class members compensatory, consequential, and general damages, including nominal damages as appropriate, for each count as allowed by law in an amount to be determined at trial;

D. That the Court award statutory damages, trebled, and/or punitive or exemplary damages, to the extent permitted by law;

E. That the Court order disgorgement and restitution of all earnings, profits, compensation, and benefits received by UHG as a result of their unlawful acts, omissions, and practices;

F. That Plaintiff be granted the declaratory and injunctive relief sought herein;

G. That the Court award to Plaintiff the costs and disbursements of the action, along with reasonable attorneys' fees, costs, and expenses; and

H. That the Court award pre-and post-judgment interest at the maximum legal rate and all such other relief as it deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands a jury trial in the instant action.

Dated: March 4, 2024

By:/s/ *E. Michelle Drake*
E. Michelle Drake
BERGER MONTAGUE
1229 Tyler Street NE, Suite 205
Minneapolis, MN 55413
Telephone: (612) 594-5933
emdrake@bm.net

Mark B. DeSanto*
BERGER MONTAGUE
1818 Market Street, Suite 3600
Philadelphia, PA 19103
Telephone: (215) 875-3046
mdesanto@bm.net

Norman E. Siegel*

J. Austin Moore*
Stefon J. David*
STUEVE SIEGEL HANSON LLP
460 Nichols Road, Suite 200
Kansas City, Missouri 64112
Telephone: (816) 714-7100
siegel@stuevesiegel.com
moore@stuevesiegel.com
david@stuevesiegel.com
**Pro Hac Vice Forthcoming*

Counsel for Plaintiff and the Class